I, MICHAEL W. FAHEY, state:

INTRODUCTION

1. I submit this affidavit in support of an application for a criminal complaint charging Joseph T. Kukstis, a 29-year-old resident of Plymouth, Massachusetts, with stalking in violation of 18 U.S.C. § 2261A ("the Stalking Offense").[1]

2. This affidavit also requests the issuance of a warrant under Fed. R. Crim. P. 41 to search any Apple iPhone possessed by Joseph T. Kukstis for evidence, fruits, and instrumentalities of both the Stalking Offense and of unauthorized access to protected computers in violation of 18 U.S.C. § 1030(a)(2)(C) (together with the Stalking Offense, "the Target Offenses").[2]

---

[1] 18 U.S.C. § 2261A provides, in pertinent part:

> Whoever —
>
> (2) with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that—
>
> (A) places that person in reasonable fear of the death of or serious bodily injury to [that person, an immediate family member, or a spouse or intimate partner of that person]; or
>
> (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to [that person, an immediate family member, or a spouse or intimate partner of that person]

[commits a felony].

[2] 18 U.S.C. § 1030 provides, in pertinent part:

> (a) Whoever — …

3. The investigation to date provides probable cause to believe that between at least as early as September 2015 and in or about October 2017, Kukstis targeted Victim 1, a 30-year-old resident of eastern Massachusetts, with an anonymous harassment campaign that was intended to cause and did cause Victim 1 substantial emotional distress.

4. As set forth below, Kukstis' course of conduct included: (1) sending Victim 1 hundreds of degrading text messages, many of which urged her to kill herself; (2) putting Victim 1 in fear that her harasser was coming to her home; (3) sending private, intimate pictures of Victim 1 to her friends and acquaintances through a "spoofed" Instagram account he created in Victim 1's name; (4) harassing friends of Victim 1 who Kukstis believed were romantically involved with her; and (5) attempting to obtain or obtaining unauthorized access to Victim 1's social media accounts.

5. Kukstis, who dated Victim 1 on and off beginning in or about November 2015, anonymously stalked Victim 1 both while he was dating her and after Victim 1 ended their relationship. To deflect suspicion, Kukstis sent himself harassing messages that he then shared with Victim 1.

6. In a January 22, 2018 e-mail from an account in his own name that he used to communicate with Victim 1, Kukstis appears to have admitted to being Victim 1's stalker,

---

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— …

(C) information from any protected computer; …

(c)(2)(B) [commits a felony punishable by imprisonment for not more than five years if]

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State….

writing to her, "it was me the entire time, I hate myself for it."

AGENT BACKGROUND

7. I have been a Special Agent with the Department of Homeland Security's Federal Protective Service for approximately 15 years. Since July 2017, I have been assigned as a Task Force Officer to the Federal Bureau of Investigation ("FBI") Cyber Task Force in the FBI's Boston office. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

8. In these roles, I have received training in the investigation of violations of federal law, to include computer-facilitated crime, and I have participated in numerous investigations as both a case agent and as an assistant to other agents. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, and electronically stored information. I have a bachelor of science degree in criminal justice from Northeastern University.

9. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and search warrant and does not set forth all of my knowledge about this matter.

ELECTRONIC COMMUNICATIONS SERVICES

10. Based on the investigation to date, I am aware that Gogii, Inc. is an electronic communication service headquartered in Marina del Ray, California that offers textPlus, a free messaging application for cell phones. textPlus enables subscribers to obtain a phone number different from the phone number assigned by their cellular carrier, and to use that phone number to send text, image, and video messages. textPlus does not require that subscribers use true names to register messaging accounts or verify all information provided at registration. textPlus accordingly permits a degree of anonymity to those subscribers who want it.

11. Based on the investigation to date, I am also aware that Instagram, LLC ("Instagram") is an electronic communications service headquartered in Menlo Park, California. Instagram, which is owned by Facebook, Inc. ("Facebook"), offers its subscribers the ability create accounts that can be used to share photos, videos, and messages with others.

PROBABLE CAUSE TO BELIEVE THAT FEDERAL CRIMES WERE COMMITTED

Victim 1

12. On November 9, 2017, FBI investigators met with Victim 1, who reported that since approximately September 2015, Victim 1 had been receiving harassing, threatening, and sexually explicit communications and images by e-mail, text message, and through other social media.

13. Initially, Victim 1 received text messages from someone claiming to be her friend, "Jeff." The messages quickly became sexual in nature, but Victim 1 could not determine who "Jeff" was.

14. Victim 1 reported that the sender frequently changed the phone numbers from which the communications originated and would sometimes use other social media platforms to communicate with her, including Facebook, Instagram, Snapchat, OK Cupid, and Tinder. The messages and images that Victim 1 received were graphic and frequently discussed sensitive personal information, which suggested to Victim 1 that the sender may have had access to her e-mail or other social media accounts and had been monitoring her communications with others.

15. Both Victim 1 and approximately five of Victim 1's acquaintances received nude images of Victim 1 from an Instagram account that used Victim 1's first and last name and the middle initial "x." Victim 1 believes the nude images were taken from another of her social media accounts where they were not available for friends or the public to see.

16. Victim 1 also received messages urging her to commit suicide and threatening harm to her intimate partners, as well as more veiled threats. On one occasion in or about March 2017, Victim 1 received a text containing her current address and the comment "see you soon." These messages caused Victim 1 enough distress that she went to the Boston Police Department to report the harassment and to request that officers accompany her back to her home to ensure her safety.

17. [redacted]

18. Victim 1 reported that the harassment had other impacts on her life. [redacted] She felt that she was being emotionally manipulated, felt powerless, and questions what she did that was so bad to deserve this treatment. Her harasser told her that they "would try and ruin every relationship in your life," which made her feel that they had taken her life away and knew where she was. Victim 1

resorted to disabling her phone so that she could sleep without being woken up in the middle of the night by harassing messages.

Harassing Text Messages

19. Victim 1 gave FBI investigators screen shots of some of the harassing text messages she received. Victim 1 also gave investigators one of the cell phones on which she had received a substantial number of the harassing communications.

20. The screen shots and the contents of Victim 1's cell phone were consistent with her report to investigators. They included the March 2017 text message that contained Victim 1's address (left) and the statement "see you soon," and another message degrading Victim 1 and urging her to kill herself (right):

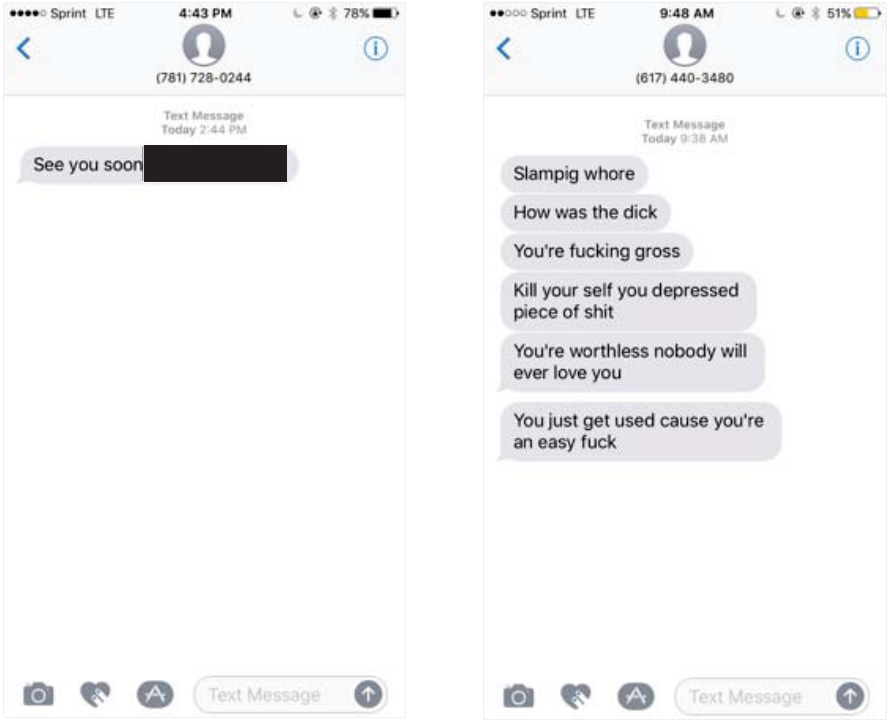

Figure 1: Screenshots of harassing text messages on Victim 1's cell phone, March 2017.

21. Victim 1 reported receiving another message, on or about March 13, 2017, after having changed phone numbers to get away from her harasser. It simply stated:

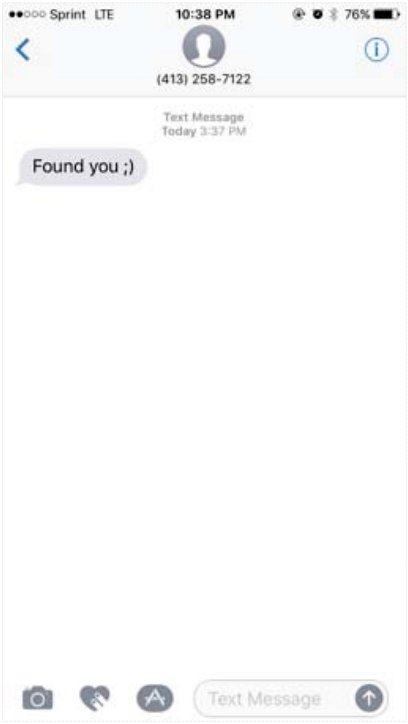

Figure 2: A screenshot of a text on Victim 1's cell phone, after she reported changing her number.

22. The harassment continued for months afterward. For example, a series of May 28, 2017 messages (left) repeated similar threats, while one May 20, 2017 text message[3] (right) expressly acknowledged that the harasser knew that Victim 1 was "living in fear:"

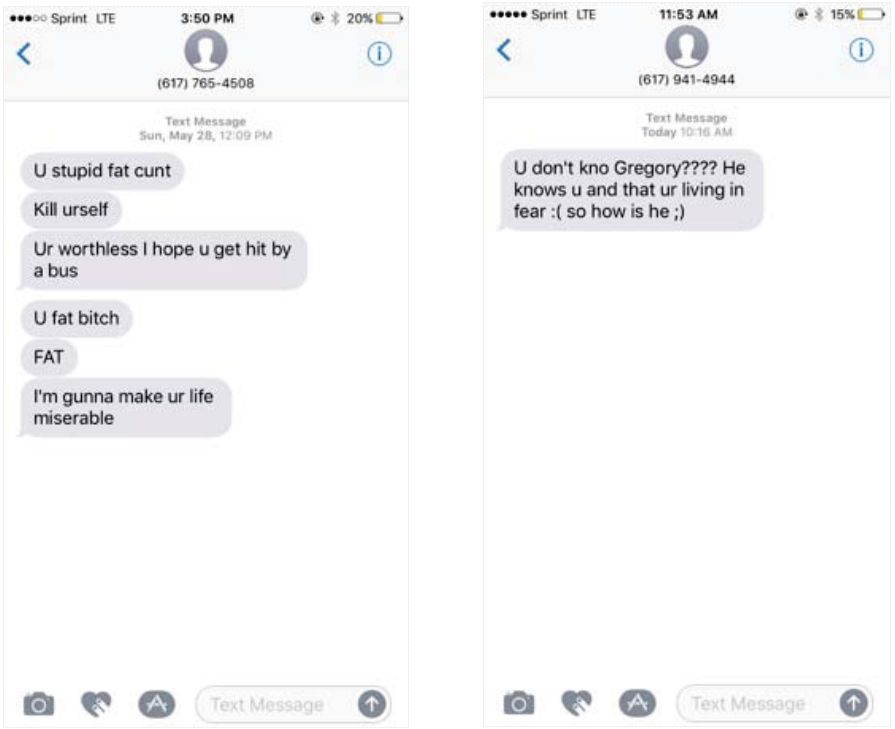

Figure 3: Screenshots of harassing messages on Victim 1's cell phone from May 28, 2017 (left) and May 20, 2017 (right).

23. On May 2, 2017, the harasser texted Victim 1 stating his intent in response to her plea to know his "end game," replying simply "there's no end game just to make u all miserable." When Victim 1 responded that "Your life is miserable," he answered "not as miserable as I'm making urs and his [and] alll the people around you."

24. Victim 1's own text messages to her friends and family make clear the impact that the harassment had on her life:

a. On January 6, 2017, Victim 1 wrote, "I got a dick pic text this morning

[3] I am aware that "Gregory" was a friend of Victim 1's with whom she communicated over social media.

from stalker."

b. On January 10, 2017, she wrote, "the harasser keeps calling me in the middle of the night … so its def time to get a new number … maybe a new phone too…."

c. On March 24, 2017, Victim 1 wrote to a friend, "So the anonymous harasser just said they were coming to my address. I have to goto the cops." Victim 1's mother wrote in response, "I am so worried" and instructed Victim 1 not to stay at her house that night.

d. On May 2, 2017, Victim 1 told a friend that her harasser was "ruining friendships everyone that gets involved is sketched out and stops being my friend."

textPlus

25. The investigation quickly focused on the phone numbers from which the threatening communications originated.

26. A forensic consultant that Victim 1 retained had reported that the majority of the harassing communications had originated from telephone numbers associated with textPlus.

27. Between January and March 2018, investigators obtained records from textPlus that included subscriber information, Internet Protocol address logs, and message content for textPlus phone numbers that either appeared as the originating phone number in screen shots of the harassing messages to Victim 1, were identified by Victim 1's forensic consultant as having sent harassing messages to Victim 1 in the past, or that FBI review of Victim 1's phone showed to have been used to send harassing messages ("the Target textPlus Accounts").

28. The textPlus subscriber information associated with the Target textPlus Accounts appeared to be purposely and largely false. For example, more than 15 of the 28 registration e-mail addresses for the Target textPlus Accounts contained a variant of the subscriber e-mail address "cunt##@aol.com," with "##" representing two random digits. The usernames and registration e-mail addresses for these 15 accounts included:

Created	First	Last	Handle	E-Mail	Last Use
6/4/17	Ccc	Bvvv	CCCBVVV-1	Cunt70@aol.com	11/10/17
5/26/17	Cam	X	CAMX-1	Cunt66@aol.com	5/28/17
5/22/17	Cuntt	Ttt	CUNTTTTT-1	Cunt60@aol.com	11/5/17
5/20/17	Cun	Tt	CUNTT-1	Cunt56@aol.com	5/21/17
5/10/17	C	Unnn	CUNNN-1	Cunt50@aol.com	11/5/17
5/8/17	Cc	Uuu	CCUUU-1	Cunt46@aol.com	5/9/17
5/28/17	Cunt	Cc	CUNTCC-1	Cunt67@aol.com	6/4/17
5/9/17	C	Units	CUNITS-1	Cunt47@aol.com	5/20/17
5/1/17	C	Nation	CNATION-1	Cunt42@aol.com	6/5/17
3/18/17	C	M	CM-124	Cunt36@aol.com	4/8/17
3/13/17	Cunt	Red	CUNTRED-1	Cunt33@aol.com	11/10/17
1/11/17	JOHN	F	JOHNF48	Cunt24@aol.com	3/13/17
6/25/17	Cccc	Hhhh	CCCCHHHH-4	Cunt82@aol.com	6/25/17
7/13/17	Cccc	Uuuu	CCCUUUU-1	Cunt96@aol.com	7/20/17
7/20/17	N	Gggg	NGGGG-1	Cunt1@aol.com	7/26/17

Table 1: textPlus accounts used to harass Victim 1, created with email addresses of the form "cunt##@aol.com."

IP Links to Kukstis

29. Notably, IP addresses associated with access to and use of the Target textPlus Accounts match IP addresses that have been used to log in to social media accounts controlled by Kukstis.

30. For example, on June 5, 2017,[4] between 15:48:19 (GMT) and 16:07:09 (GMT), the textPlus number 617-409-7924 ("the 7924 Number") sent the five SMS messages below to Victim 1's phone:

SMS:

543	+16174097924	N/A	05/06/2017 15:48:19 (GMT)		Read	Inbox	Phone	Incoming	How many dicks have u sucked
544	+16174097924	N/A	05/06/2017 15:48:20 (GMT)		Read	Inbox	Phone	Incoming	Sendin all ur naked pics to joe ;)
545	+16174097924	N/A	05/06/2017 15:57:59 (GMT)		Read	Inbox	Phone	Incoming	I'm gunna ruin ur life
546	+16174097924	N/A	05/06/2017 16:07:09 (GMT)		Read	Inbox	Phone	Incoming	Did u spread ur legs
547	+16174097924	N/A	05/06/2017 16:29:08 (GMT)		Read	Inbox	Phone	Incoming	Wat wud ur mom think of these naked pics

Table 2: Text messages sent from textPlus number 617-409-7924 to Victim 1's phone

31. According to textPlus records, the user account corresponding to the 7924 Number, CCCBVVV-1, was created on June 4, 2017 with the associated user email cunt70@aol.com. textPlus allocated the 7924 Number to this account on June 5, 2017 at 15:07 (GMT), approximately 40 minutes before these messages were sent to Victim 1.

32. Between 15:03 (GMT) and 16:29:08 (GMT) that day—the time of the last harassing message above—the only IP address to access the textPlus account that sent these messages was 73.159.127.236 ("the 127.236 IP Address").

33. According to records investigators obtained from Apple, Inc., at almost exactly the same time that day, between approximately 14:57 (GMT) and 15:23 (GMT), an iTunes account in the name of Joseph Kukstis (of Plymouth, Massachusetts) was updated from the 127.236 IP Address— the same IP address used to send the harassing messages in paragraph 320 to Victim 1 over textPlus.

[4] The forensic software that created the report below uses the European standard to organize dates. Under this standard, 05/06/2017 is June 5, 2017, not May 6, 2017.

34. The same 127.236 IP Address was also used that day during the same period, between 15:13 (GMT) and 17:48 (GMT), to log in six times to an Instagram account registered to a Gmail account that Kukstis controlled. The 127.236 IP Address was also used to access this Instagram account approximately 48 times overall in May and June 2017.

35. Because the 127.236 IP Address was used on June 5, 2017 to send threatening messages to Victim 1 over textPlus and to communicate with both Apple and Instagram regarding Kukstis' accounts with those providers, there is probable cause to believe that Kukstis sent the offending messages on June 5, 2017, and that he was involved in stalking Victim 1.

36. This conclusion is reinforced by an analysis of IP addresses associated with the access to and use of all of the Target textPlus Accounts. That analysis reveals that a single IP address, 73.69.73.32 ("the 73.32 IP Address"), accounted for approximately 4244 out of approximately 9718 of the total IP address connections to the Target textPlus Accounts, or nearly 44 percent.

37. The same 73.32 IP Address features prominently in Apple's records related to Kukstis' accounts— it was used: (a) six times between June 14, 2016 and May 23, 2017 to create billing profiles; (b) approximately 89 times between June 14, 2016 and October 20, 2017 for iTunes orders; and (c) approximately 1,250 times between May 24, 2016 and May 24, 2017 for iTunes updates.

38. The 73.32 IP Address was similarly used to access Kukstis' Instagram account more than 400 times between January and May 2017.

39. Together, the 127.236 IP Address and the 73.32 IP Address described above accounted for approximately two-thirds of the total IP traffic to the Target textPlus Accounts.

The Spoofed Instagram Account

40. A review of the forensic image of Victim 1's phone also revealed, as Victim 1 had reported, that Victim 1's harasser had used an Instagram account in her name to send offensive messages and nude photographs of Victim 1 to her friends.

41. Specifically, on June 2, 2017 at approximately 9:49 a.m. (EDT), an individual Victim 1 had dated years earlier ("Friend 1") sent her an image by message asking, "Is that you?" The image featured a photograph of Victim 1's face and Victim 1's first and last names separated by the letter x, both of which made it appear as if Victim 1had sent the offensive message it contained.

Figure 4: Message sent from the Spoofed Instagram Account to Friend 1.

42. Two days later, on June 4, 2017 at 10:32 a.m. (EDT), Friend 1 sent Victim 1 another image by instant message. The image was also a screenshot of a message from the Spoofed Instagram Account that bore Victim 1's face and name. The message, however, contained a photograph depicting Victim 1 engaged in a sexual act. Victim 1 has reported to me that the photograph was taken years earlier and that she had shared it with only one person, not Kukstis, in a private Facebook message.

43. Victim 1 and Friend 1 exchanged the following messages:

Victim 1: WHAT THE FUCK
HOLY SHIT
They really did hack my phone
Jesus fucking Christ

Friend 1: I really don't get why this is happening.

Victim 1: It's been happening for almost two years.
It's getting worse now.

Friend 1: Yea I know.

Victim 1: I don't get it either.
There's nothing I could have possibly done to have this happen
I'm not a bad person.

Friend 1: No you're not

Victim 1: I've made mistakes but everyone has.

Friend 1: And I really don't get why im part of it.

Victim 1: Cus you dated me
And they know that

Friend 1: Yea but so what. What does sending me that video accomplish

Victim 1: Idk
Did you report the IG

Friend 1: Yea I did last time too
I'm sorry

Victim 1: Fuck this
I feel so violated
I can't believe they sent that.

…

Victim 1: I don't want people I know seeing that stuff

44. On June 5, 2017, Friend 1 forwarded to Victim 1 a screen shot of a final message to Friend 1 from the Spoofed Instagram Account:

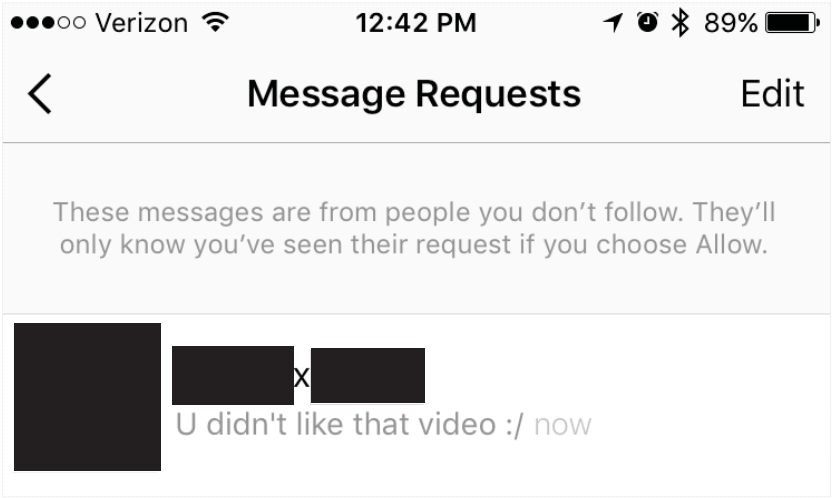

Figure 5: Another message from the Spoofed Instagram Account to Friend 1.

45. Investigators obtained records from Instagram regarding the Spoofed Instagram Account, which indicate that the account was established with the registered e-mail cunt44@aol.com. As noted above, email addresses using this naming convention (i.e., cunt##@aol.com) were used to create at least 15 textPlus accounts used to harass Victim 1. Because there is probable cause to believe that Kukstis created those 15 "cunt##@aol.com" textPlus accounts, there is also probable cause to believe that he created and used the cunt44@aol.com address in connection with the Spoofed Instagram Account.

46. Indeed, Instagram's records show that the Spoofed Instagram Account was registered on May 6, 2017 at 03:22:47 (UTC) from the 73.32 IP Address—the same IP Address that investigators have already linked to approximately 1,700 IP address connections to Kukstis' Apple and Instagram accounts. See paragraphs 37 and 38 above.

47. Records from Instagram also show that the 73.32 IP Address was used on May 6, 2017 at 3:25:52 (UTC) to access Kukstis' Instagram account—just over three minutes after it

was used to establish the Spoofed Instagram Account. Apple's records similarly show iTunes update activity over the 73.32 IP Address on Kukstis' account there at 3:54:10 (UTC), approximately one half-hour after the 73.32 IP Address was used to create the Spoofed Instagram Account.

48. There is accordingly probable cause to believe that Kukstis controlled the Spoofed Instagram Account and used it to distribute harassing communications to Friend 1 and others in an effort to harass Victim 1 in early June 2017.

Kukstis Pretended To Be a Victim Himself

49. Messages between Kukstis and Victim 1 in May and June 2017 show that Kukstis sometimes sent himself harassing messages by textPlus. He then shared these messages with Victim 1 so that she would believe that someone else was harassing them both.

50. For example, on May 10, 2017, beginning at 12:22 a.m., the textPlus account (617) 245-0198 was used to generate the messages below and to send them to [redacted]5793, a telephone number that Kukstis both used to communicate with Victim 1 and registered with Apple in connection with his account there:

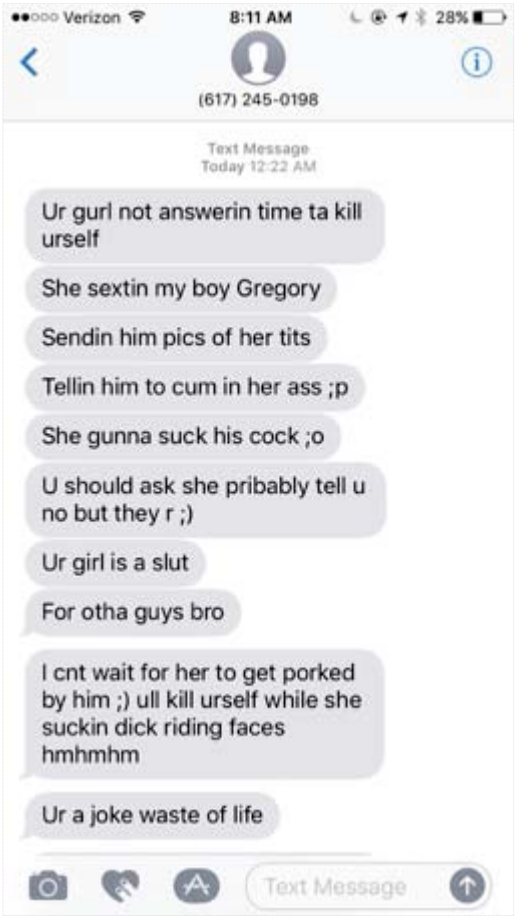

Figure 6: An image from Victim 1's cell phone containing messages Kukstis created using the telephone number [redacted]5793.

51. This image/screenshot, taken at 8:11 a.m. according to the time that appears in the image, was found on Victim 1's phone. According to the activity log in Victim 1's phone, Kukstis messaged her a minute later, at 8:12 a.m. There is accordingly probable cause to believe that Kukstis created the screenshot and immediately messaged it to Victim 1 as "proof" that he was being harassed.

52. Records from textPlus, however, provide probable cause to believe that it was Kukstis who sent these offensive messages to himself. On May 10, 2017, the only IP address to access the (617) 245-0198 textPlus account—the account that sent the messages to Kukstis' [redacted]5793 phone number—was the 73.32 IP Address. As noted above, this is the IP address that Kukstis used to access his own Instagram account more than 400 times, to create the

Spoofed Instagram Account, and to update his Apple iTunes account.

53. As another example, on May 2, 2017 at 1:44 p.m., the following messages were sent from (781) 214-7686—a textPlus number—to the above-described [redacted]5793 phone number associated with Kukstis:

Figure 7: A screenshot retrieved from Victim 1's Gmail account, sent to her by Kukstis on May 2, 2017.

54. At 1:52 p.m., Kukstis sent this screenshot by e-mail to Victim 1, stating: "Now it's my life cool I tried texting a pic but it's green wouldn't send. / Sent from my iPhone."

55. Records from textPlus, however, show that the text messages above were sent from a textPlus account associated with the email address cunt42@aol.com. Records show that the only IP address to access that textPlus account between May 1, 2017 and May 4, 2017 was Kukstis' 73.32 IP Address.

56. There is accordingly probable cause to believe that Kukstis harassed himself and shared these fabricated messages with Victim 1, all to suggest that someone else was her

harasser. These messages had the desired effect, with Victim 1 texting Kukstis on May 9, 2017 that "The fact they're FUCking with you pisses me off."

57. Review of Victim 1's phone also revealed that while Kukstis was texting Victim 1 in a purported effort to console her, he was sometimes harassing her at the same from anonymous textPlus accounts.

58. This behavior is consistent with Kukstis' other attempts to deceive Victim 1. For example, in a May 20, 2017 e-mail, days after he repeatedly sent himself harassing messages by textPlus, Kukstis wrote Victim 1: "be safe I care about you you're precious cargo *whoever is doing this is a coward and it's annoying*" (emphasis supplied).

Harassment of Others

59. As noted above in paragraphs 40 to 48, Kukstis used the Spoofed Instagram Account to distribute private, intimate pictures of Victim 1 to others, and in doing so harassed both Friend 1 and Victim 1.

60. In other instances, Kukstis harassed men via textPlus who were acquainted with Victim 1.

61. For example, on May 10, 2017, Friend 2 communicated with Victim 1 about receiving harassing messages, texting: "seriously don't worry about it. It doesn't bother me in the least. I'm hoping so much they keep trying to contact me so I can continue to help."

62. In another instance, on approximately June 25, 2017, a then romantic interest of Victim 1 (Friend 3) received a series of anonymous social media messages describing parts of Victim 1's anatomy and claiming to have had sex with Victim 1 in the back room of a grocery store. This led Friend 3 to attach a screen shot of the exchange to a text message to Victim 1, asking "Did you do this?"

Social Media Access

63. Because her harasser frequently knew, commented on, and shared images of Victim 1's life that she had not made public, Victim 1 believed that her harasser had access without her permission to one or more of Victim 1's social media accounts.

64. The investigation to date provides probable cause to believe that Kukstis did obtain or attempt to obtain unauthorized access to Victim 1's social media accounts.

65. In one anonymous message dated May 2, 2017, Kukstis claimed through one of the textPlus accounts he used to harass himself to have "been on [Victim 1's] Instagram haha," to which Victim 1 responded, "which is private so that makes you someone I know."

66. Victim 1 also gave investigators screen shots dating between July 2016 and October 2017 evidencing attempts to access, reset passwords for, or delete her accounts at various social media websites, including Instagram, Sprint, OKCupid, Facebook, and Snapchat.

67. Victim 1 also reported receiving a communication from Facebook during the late summer of 2016 advising that her account had been accessed by a device in Plymouth, Massachusetts, where Kukstis resides. Victim 1 confronted Kukstis, who denied accessing her account (although he would later tell her that he had done so).

68. Victim 1's records from Apple also show dozens of attempts to reset the password on her Apple iCloud account in both February 2017 and June 2017. These attempts originated from the 73.32 IP Address and the 127.236 IP Address, both of which have been identified above as IP addresses that Kukstis used during his harassment campaign targeting Victim 1.

69. For all of these reasons, and especially in light of Kukstis' e-mailed statement to Victim 1 on January 22, 2018, there is probable cause to believe that Kukstis stalked Victim 1

and that he committed the Target Offenses while doing so.[5]

PROBABLE CAUSE TO BELIEVE THAT KUKSTIS' CELL PHONE WILL CONTAIN EVIDENCE, FRUITS, AND INSTRUMENTALITIES OF THE TARGET OFFENSES

70. Records from textPlus and Apple reveal that Kukstis connected to Apple and textPlus' services during his harassment campaign, and since at least as early as January 11, 2017, using an Apple iPhone 7.

71. Specifically, Apple records regarding Kukstis' Apple ID show that it has been accessed between approximately December 2017 as February 14, 2018 from an "iPhone9,1," which open source databases indicate is a device type that corresponds to an Apple iPhone 7.

72. textPlus records similarly show, between January 11, 2017 and June 7, 2017, the vast majority of device connections to textPlus accounts over the Target textPlus Accounts that Kukstis used to harass Victim 1 originated with an "iPhone 9,1" (i.e., an iPhone 7).

73. Additionally, in September 2017, connections to the Target textPlus Accounts continued to be associated with an "iPhone 9,1" but instead used the IP address 98.110.234.40 and the listed network "WIFI." Verizon records show that 98.110.234.40 was an IP addressed assigned to the Kukstis residence (with Kukstis' mother the named subscriber) in Plymouth, Massachusetts.

74. The above records establishing Kukstis' use of an iPhone 7 to harass Victim 1 are consistent with Victim 1's memory of her time with Kukstis. She reported that Kukstis regularly

[5] The investigation has also revealed other instances in which Kukstis-controlled textPlus accounts have been used to harass others. On September 26, 2017, for example, a textPlus account—registered to cunt100@aol.com and accessed from two of Kukstis' residential IP addresses—was used to send messages impersonating a 24-year-old woman who had died in a car crash months earlier. The messages, sent to the dead woman's friends, included "Sry I sent myself thru my car windshield" and "It's [Name] I'm dead."

used an iPhone to which he had upgraded during their relationship. In fact, nearly all of the e-mail communications that Kukstis had with Victim 1 in his own name stated in an automated footer that they were "sent from my iPhone."

75. There is accordingly probable cause to believe that Kukstis' cell phone was an instrumentality of the Target Offenses and will contain evidence of those offenses.

76. There is also probable cause to believe that Kukstis carries his cell phone on his person. Based on my training and experience as an investigator, I am aware that people typically carry cell phones with them inside and outside their homes – convenient, mobile access to the cellular network (and the Internet beyond it) is one of the principal advantages of a cell phone over a landline connection. In fact, on March 26, 2018, FBI personnel saw Kukstis walking a dog near his home. They photographed him wearing earphones that I believe based on their appearance to be Apple-branded. The earphone cord connected to an unseen device, likely an iPhone, in Kukstis' pants pocket. Account records gathered during the course of the investigation, which show access to social media networks over both wireless and residential IP addresses at various times of the day and night, are also consistent his regularly carrying a cell phone.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

77. Based on my training, experience, and information provided by other law enforcement officers, I know that many smartphones (which are included in Attachment B to the proposed search warrant's definition of "hardware") can now function essentially as small computers. Apple iPhones, such as Kukstis' cell phone, are a type of smartphone. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a

vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

78. As set forth above, there is probable cause to believe that Kukstis used his iPhone to connect to textPlus, Instagram, and Apple to commit the Target Offenses by sending text messages and images targeting Victim 1 and attempting to access her social media accounts.

79. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from

operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

80. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process

can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements ─ analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

81. For many of these reasons, Kukstis may possess computer equipment whose use in the crimes or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B to the proposed search warrant are of the type that might be

found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

UNLOCKING AN APPLE DEVICE USING TOUCH ID FEATURE

82. As described above, there is probable cause to believe that Kukstis' cell phone is an Apple brand device, likely an iPhone 7.

83. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads, offer their users the ability to unlock the device via the use of a fingerprint in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

84. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a passcode, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

85. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked

via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

86. The passcode that would unlock Kukstis' iPhone is not known to law enforcement. Thus, it will likely be necessary to press Kukstis' finger(s) to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the iPhone via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

87. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of Joseph Kukstis to the Touch ID sensor of any iPhone in his possession for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

CONCLUSION

88. Based on the information described above, there is probable cause to believe that Joseph T. Kukstis committed the Stalking Offense. A complaint and warrant for his arrest should issue.

89. There is also probable cause to believe that he will possess a cell phone on his person, and that that phone was an instrumentality of and will contain evidence of the Target Offenses. A search warrant for the phone in his possession should accordingly also issue.

90. Because the investigation is not public and will continue in the days leading up to

Kukstis' arrest, and in order to prevent the destruction of evidence or harassment of victims that could result from Kukstis or others becoming aware of this investigation, the government respectfully requests that the Court seal the search warrant, the arrest warrant, the complaint, and the application materials in support of them except as is necessary to execute the warrants.

Respectfully submitted,

MICHAEL W. FAHEY
Special Agent/Task Force Officer
Federal Protective Service/
Federal Bureau of Investigation

Subscribed and sworn to before me
on April 2, 2018

DAVID H. HENNESSY
United States Magistrate Judge